

Máte už svůj Let's Encrypt certifikát?



Ing. Tomáš Hála
IT Security & Operations manager
ACTIVE 24, s.r.o.
@tomashala

1. června 2016
Internet a Technologie 16



Už jste někdy šifrovali?

Hlava II **Nepovolené internetové hry**

§ 82 **Blokace nepovolených internetových her**

(1) Poskytovatelé připojení k internetu na území České republiky jsou povinni zamezit v přístupu k internetovým stránkám uvedeným na seznamu internetových stránek s nepovolenými internetovými hrami (dále jen „seznam nepovolených internetových her“).

Svobodný INTERNET



active 24

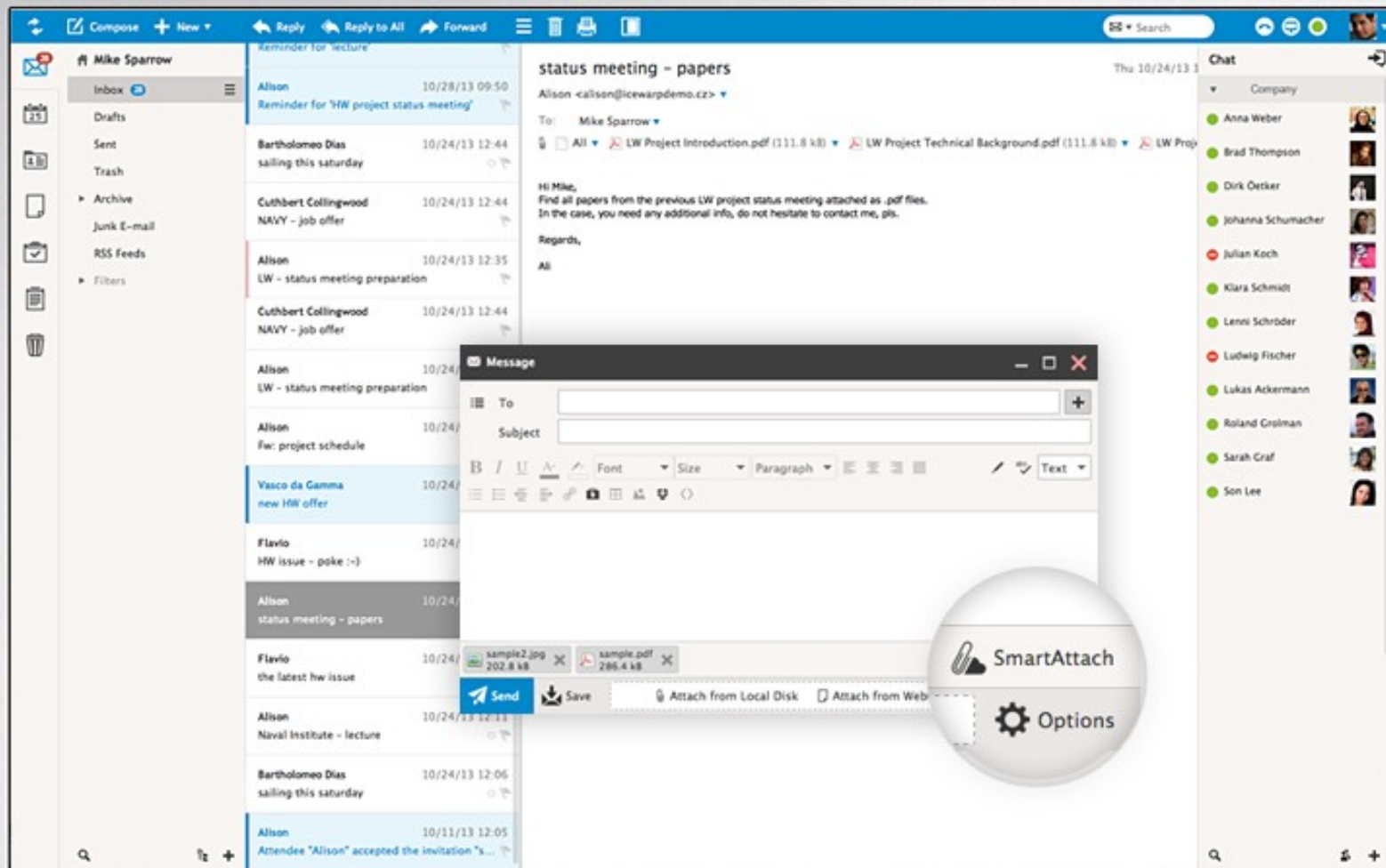
Co jsme Ioni slibovali

Co jsme loni slibovali

- HTTPS na všech webech by default
- instalace a provoz SSL zcela zdarma
- samoobslužná instalace certifikátů
- podpora SPDY a následně HTTP/2
- podpora SSL na IPv6
- SSL terminace na reverzní proxy NGINX

Splněno! A čím dalším jsme se zabývali poslední rok?







O čem že je tato přednáška?



Let's Encrypt

Ale proč vlastně komunikaci šifrovat?

How?

Exploit the target transparently by injecting a browser-based exploit while he's surfing the web (http)

]HackingTeam[

AT&T caught injecting extra ads on airport WiFi hotspot

1

Adam Westlake - Aug 26, 2015

Twitter 52

Facebook 23

Google

Reddit



It seems **AT&T** may be tampering with mobile users' internet traffic for their own benefit on their "free" public WiFi hotspots. The company's hotspot at the Dulles International Airport in Virginia was found to be using ad-injecting code to deliver more advertisements to users while they browse the web. Stanford lawyer and computer scientist Jonathan Mayer made the discovery, detailing the tactic on [his blog Web Policy](#).



"Eric" "Mill"

@konklone



+ Sledovat

Wikipedia's decision to enforce HTTPS is now pitting them against Russian censors, who want the HTTPS turned off:
theguardian.com/world/2015/aug...

Zobrazit překlad



Википедия

Свободная энциклопедия

Заглавная страница

Рубрикация

Указатель А — Я

Избранные статьи

Случайная статья

Заглавная

Обсуждение

Чит



Добро пожаловать в Википедию

свободную энциклопедию, которую может редактировать каждый

Сейчас в Википедии **1 248 170 статей** на русском языке

[Создать статью \(с помощником\)](#)

Russia briefly bans Wikipedia over page relating to drug use

Court ordered ban on page about charas, an Indian form of hashish, but some Russian users found entire site blocked due to secure https protocol

theguardian.com



Jak jsme Let's Encrypt implementovali v ACTIVE 24



Jak jsme Let's Encrypt implementovali v ACTIVE 24

- na každou doménu na našem Linux hostingu
- zdarma a automaticky krátce po zřízení hostingu
- včetně aliasů, mimo wildcard (např. *.active24.cz)
- samozřejmě automatické obnovy
- při zřízení self-signed, následně nahrazování pomocí LE
- možnost nahradit certifikátem komerčním
- služba typu „best-effort“
- vybrali jsme acme.sh klient



A co vy, máte už svůj Let's Encrypt certifikát?



WANTED

- senior J2EE programátor
- BSD server adminisztrátor



Děkuji za pozornost!

www.active24.cz
blog.active24.cz
@active24cz
@tomashala

